IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF APPLE ACCOUNT(S) INFORMATION ASSOCIATED WITH TAUREAN VENABLE, CELLULAR PHONE NUMBER 202-733-0357 THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	)))))))	Case No. 1:20-SW-1517 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Stacey Ivie, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple Account(s) and Apple ID(s) associated with TAUREAN VENABLE, cellular phone number 202-733-0357, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Police Detective with the Alexandria Police Department, (APD), where I have been employed since 2002. During my employment with APD, I have been a detective for over fourteen years and have investigated numerous types of crimes, including but not limited to fraud, money laundering, narcotics and organized crime. I have conducted and/or participated in numerous narcotics investigations resulting in the arrest and/or conviction of drug distributors and

the seizure of quantities of controlled substances and other evidence affiliated with drug distribution. I have also received specialized training in areas to include the preparation and execution of federal and state search warrants. The Drug Enforcement Administration ("DEA") also concurrently deputizes me as a DEA Task Force Officer. Since November 19, 2011, I have been assigned to the High Intensity Drug Trafficking Area Task Force, Northern Virginia Financial Initiative in Annandale, Virginia.

3. While with the DEA and APD, I have participated in the investigation of narcotics traffickers and possessors. Many of these investigations led to the arrest and conviction of narcotics dealers and money launderers. In the course of conducting these investigations, I have used several different kinds of investigative techniques, including, but not limited to: interviewing informants and cooperating sources; conducting physical surveillance; conducting short-term and long-term undercover operations, including reverse undercover operations; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification data; conducting court-authorized electronic surveillance; preparing and executing search warrants, which have led to substantial seizures of narcotics, firearms, contraband, and drug related assets; and, the analysis of financial documents and records. I know through training and experience that individuals involved in narcotics trafficking frequently use cellular telephones to further their illegal activities (a) as the phones allow them to stay in contact with one another without restricting them to a fixed location where they might be the subject of physical surveillance by law enforcement authorities; and (b) because they erroneously believe that the interception of cellular communications is impossible or at least more difficult than interception of land-line telephones. Further, drug traffickers rarely expressly refer to controlled substances by name while communicating over telecommunications devices (to conceal

the true nature of their illegal activities and to avoid detection by law enforcement, they refer to the drugs and drug quantities using seemingly innocent terms). I also know through training and experience that drug traffickers often carry firearms to protect their illegal narcotics and the proceeds from illegal narcotic sales.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841(a) and 846, conspiracy to distribute controlled substances, are located within the items described in Attachment A. There is also probable cause to believe that the electronically stored information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of additional individuals who engaged in the commission of these offenses.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. Background of the Investigation

7. In early 2020, law enforcement obtained information about subjects distributing quantities of controlled substances in the Eastern District of Virginia and elsewhere. During the

course of this investigation, law enforcement was able to seize large quantities of fentanyl and other controlled substances and obtained evidence that Taurean VENABLE, also known as "Tip" (hereinafter referred to as "VENABLE"), was conspiring with others to distribute controlled substances.

B. Law enforcement seizure of fentanyl on June 1, 2020

8. On June 1, 2020, law enforcement officers executed a search warrant at a residence in Arlington, Virginia, within the Eastern District of Virginia. During the execution of the search warrant, law enforcement found evidence consistent with the manufacturing and packaging of suspected controlled substances in almost every room of the three-bedroom apartment. White powder was prevalent throughout and covered many items. There were also numerous boxes and/or containers of corn starch, cellulose, caffeine tablets, and Magnesium Sulfate, among other materials which, based on my training and experience, are used as cutting agents by drug traffickers.

9. In the kitchen area, law enforcement located numerous mixing containers, grinders, scales, and packaging materials with suspected narcotics residue. A search of the middle island cabinet revealed an empty package displaying LFA Machines, a company that manufactures pill presses. In the kitchen garbage, officers located additional large amounts of powder,[1] along with shipping labels and several discarded tablets with markings consistent with controlled prescription tablets. Officers located a machine suspected of being used to press kilogram quantities of narcotics known as a "kilo press" in the kitchen island cabinet. In addition, officers found a blender

[1] Unless otherwise indicated, lab tests of substances found at the Arlington address are pending with the Mid-Atlantic Laboratory of the DEA.

on the kitchen counter containing a large amount of powder. On July 7, 2020, law enforcement received results of a qualitative analysis, including net weight and identification, conducted by the Mid-Atlantic Laboratory of the DEA. The analysis reflected that the contents of the blender weighed approximately 1,082 grams and was positive for fentanyl.[2]

10. The renter of the apartment was subsequently arrested and charged with drug trafficking charges. This subject (hereinafter, "CS-1") later agreed to cooperate with law enforcement.

C. Law enforcement seizure of fentanyl on June 2, 2020

11. While the search warrant was being executed on June 1, 2020 in Arlington, Virginia, officers located a vehicle associated with CS-1 parked in the garage of the apartment building.

12. A K-9, Arlo,[3] and his handler conducted a sweep of the vehicle which resulted in a positive alert by Arlo. Following the alert, this vehicle was secured and towed (followed by law enforcement) to the Arlington County Police Department's impound lot.

13. On June 2, 2020, officers obtained and executed a search warrant of this vehicle. Inside the trunk, officers found one (1) heat sealed black and clear package containing thousands of tablets with markings consistent with those of Percocet, a prescription controlled substance. Law enforcement also found two (2) heat sealed packages with shapes consistent with the

[2] Based on my training and experience, fentanyl is commonly mixed with or substituted for other opioids in counterfeit tablets purporting to be, for example, Oxycodone.

[3] "Arlo" was last certified in April 2019 to alert to the odors of substances including heroin, cocaine, and methamphetamine and is trained on a monthly basis to ensure Arlo's accuracy. Arlington County, Virginia Police Office Anatoliy Biskoup is Arlo's handler.

packaging for a kilogram of a controlled substance. One of these packages was silver and the other was clear with a visible white block with an Audi vehicle emblem imprinted on it.

14. On July 6, 2020, law enforcement received the results of a qualitative analysis, including net weight and identification, conducted by the Mid-Atlantic Laboratory of the DEA. The analysis reflected that the contents of clear heat-sealed package containing the white substance with the Audi emblem weighed 665.7 grams (without packaging) and was positive for fentanyl and xylazine. Another qualitative analysis conducted by the Mid-Atlantic Laboratory of the DEA Administration reflected the silver heat sealed package weighed 1007.0 grams (without packaging) and was positive for fentanyl. The 5,307 pills found in the trunk were also found to be a mixture or substance containing fentanyl weighing approximately 4437 grams total.

D. Historical Information Provided by CS-1

15. CS-1 is a self-admitted distributor of "Molly," heroin, and fentanyl with a prior conviction for drug distribution. CS-1 is cooperating with law enforcement in hopes of possible consideration for a sentence reduction on a pending federal drug trafficking charge. CS-1 has provided information to law enforcement that has been independently corroborated. Based on the forgoing, I consider CS-1 reliable.

16. CS-1 began manufacturing thousands of pills using fentanyl in 2019. CS-1 reported that he subsequently began purchasing large quantities of fentanyl with an unindicted co-conspirator (hereinafter referred to as UCC-1). CS-1 reported that UCC-1 was also in possession of pill presses and was attempting to make his or her own pills from fentanyl. CS-1 stated that UCC-1 maintained an apartment at 520 12th Street South in Arlington, Virginia—the same building where CS-1 lived and where the seizures occurred on June 1, 2020—that was only used to store the press and possibly controlled substances/drug proceeds. CS-1 reported UCC-1 supplied

VENABLE with large quantities of heroin and pills, which he further distributed to numerous customers in the Washington, D.C. metropolitan area. CS-1 reported that UCC-1 subsequently provided five thousand (5,000) to ten thousand (10,000) pills containing controlled substances to VENABLE via another unindicted co-conspirator (hereinafter referred to UCC-2) in the Eastern District of Virginia. From looking at the contents of CS-1's own cellular phones, CS-1 identified VENABLE's current cellular phone number as 202-733-0357.

17. Furthermore, CS-1 knew VENABLE previously conducted cocaine transactions with another unindicted co-conspirator (hereinafter referred to UCC-3). CS-1 reported that VENABLE and UCC-3 subsequently had a disagreement over twelve (12) grams of cocaine that had been "fronted" to VENABLE. CS-1 stated that VENABLE went by the nickname "Tip."

D. Historical Information Provided by CS-2

18. CS-2 is a self-admitted distributor of cocaine with a prior conviction for drug distribution. CS-2 is cooperating with law enforcement in hopes of receiving a sentence reduction on a pending federal drug trafficking charge. CS-2 has provided information to law enforcement that has been independently corroborated. Based on the forgoing, I consider CS-2 reliable.

19. CS-2 reported that VENABLE supplied CS-2 with one hundred twenty-five (125) gram quantities of cocaine in approximately 2016.

20. CS-2 reported that he purchased five hundred (500) grams of cocaine every other day for three (3) months from VENABLE beginning in June 2017. CS-2 often referred to VENABLE as "Tip."

E. Subscriber information obtained from law enforcement databases

21. A law enforcement database (Accurint) shows that phone number 202-733-0357 is affiliated with "Alphnzo VENABLE" of 520 12th Street South, Apartment 1608, Arlington, Virginia.

F. Communications between UCC-3 and VENABLE

22. Following the encounter with law enforcement in June 2020, CS-1 consented to a search of his cellular telephones, which revealed communications corroborating CS-1's statements regarding UCC-3 and their distribution of heroin and fentanyl. A search warrant was obtained for UCC-3's Apple iCloud account, which revealed communications, including iMessages, between UCC-3 and the cellular phone number, 202-733-0357, which is linked to VENABLE. The iMessages indicate that both parties were communicating using an iPhone. Therefore, I have reason to believe that these communications, and others like them, will be linked to Apple Account(s) or Apple ID(s) associated with VENABLE's cellular phone number—202-733-0357, and that information associated with those Apple Account(s) is stored on iCloud.

23. On July 2, 2019, UCC-3 and VENABLE exchanged the following messages:

DATE	FROM	MESSAGE
07/02/19	VENABLE	Tip
07/02/19	UCC-3	Bet bout to lock you in
07/02/19	VENABLE	Ok
07/02/19	VENABLE	Bro fuck with me we going run it up
07/02/19	VENABLE	I play fair
07/02/19	VENABLE	And I do what I want in my city
07/02/19	UCC-3	That's a bett my nigg we locked in I"mma fuck with you definitely keep me posted on the situation

07/02/19	VENABLE	I already got the Downtown I'm waiting on that girl
07/02/19	UCC-3	Bet that imma get with you
07/02/19	VENABLE	Ok

24. VENABLE refers to himself in this exchange as "Tip," the same nickname for him known to CS-1 and CS-2. Through my knowledge of this investigation and discussions with CS-1, during this exchange, VENABLE is advising UCC-3 that he is waiting on "girl," which is common slang for cocaine. VENABLE further states that he "play fair" which is slang for charging reasonable prices on controlled substances.

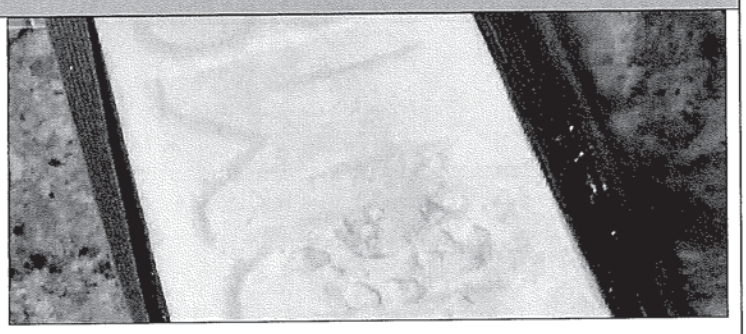
25. On July 10, 2019, UCC-3 and VENABLE exchanged the following messages:

DATE	FROM	MESSAGE
07/10/19	VENABLE	What you been up too ain't heard from you you good
07/10/19	UCC-3	Oh yeah I'm good just chilling that thang ever touch down
07/10/19	VENABLE	I'm still waiting
07/10/19	VENABLE	I been playing with that other thing
07/10/19	UCC-3	Aite imma see if my folks fuck with it let me get something small
07/10/19	VENABLE	Ok I will hit u when I get on that side

26. Through my knowledge of this investigation and discussions with CS-1, during this exchange, VENABLE advised UCC-3 that he is still waiting for a shipment and that he had "the

other thing." Based on your affiant's training and experience, "the other thing" refers to another controlled substance and UCC-3 agrees to obtain a small quantity.

27. On July 14, 2019, UCC-3 and VENABLE exchanged the following messages:

DATE	FROM	MESSAGE
07/14/19	VENABLE	
07/14/19	UCC-3	Oh yeah I just picked the bread up imma hit you when I'm back on that side
07/14/19	VENABLE	Bet
07/14/19	UCC-3	You gonna be around at like 6
07/14/19	VENABLE	Yea
07/14/19	UCC-3	Bet imma hit you
07/14/19	VENABLE	Ok

28. Through my knowledge of this investigation and discussions with CS-1, during this exchange, UCC-3 and VENABLE are agreeing to a narcotics transaction in the near future. "Bread" is common slang for money. The image that was sent by VENABLE is consistent with approximately a kilogram of cocaine or other controlled substance.

29. On July 15 and 16, 2019, UCC-3 and VENABLE exchanged the following messages:

DATE	FROM	MESSAGE
07/15/19	UCC-3	It a go! My folks fucking with it
07/15/19	VENABLE	What they say
07/16/19	VENABLE	How u looking slim
07/16/19	UCC-3	If my folks come get this joint I'll have one left
07/16/19	VENABLE	I need you to grab another one so I can show my peoples we can move it to keep the ball rolling

30. Through my knowledge of this investigation and training and experience, during this exchange, UCC-3 is reporting that his customers liked the quality of the controlled substance previously purchased. When VENABLE subsequently asks how UCC-3's sales of the controlled substances are going, UCC-3 reports that he is nearly sold out of the controlled substance. VENABLE then tells UCC-3 that he needs UCC-3 to purchase more product so that he can prove to his supplier that he is capable of moving larger amounts of the controlled substance.

31. On April 20, 2020, UCC-3 and VENABLE exchanged the following messages:

DATE	FROM	MESSAGE
04/30/20	VENABLE	Yo wasssup
04/30/20	UCC-3	Everything still the same
04/30/20	VENABLE	What that gurl
04/30/20	UCC-3	Yeah
04/30/20	VENABLE	Waiting now bruh u know them numbers high is shit now

04/30/20	UCC-3	Ohh damn I ain't know that
04/30/20	VENABLE	Bruh that shit been hard to get since shit been lock down
04/30/20	UCC-3	True I ain't even think about that

32. Through my knowledge of this investigation and training and experience, during this exchange, UCC-3 is asking VENABLE about the availability of cocaine. VENABLE related that due to Covid-19, it is currently difficult to obtain controlled substances at a reasonable price.

INFORMATION REGARDING APPLE ID AND ICloud[4]

33. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

34. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

[4] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

35. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

36. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email

addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

37. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

38. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

39. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

40. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

41. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

43. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

48. I believe that there are sufficient facts establishing probable cause to conclude that: 1) Taurean VENABLE is a drug-trafficker; and 2) that he uses iMessages generated on an

iPhone associated with cellular phone number 202-733-0357 to facilitate his drug trafficking business. I further believe that there is probable cause to believe that Taurean VENABLE, using cellular phone number 202-733-0357, is associated with Apple ID(s) and Apple Account(s), and that information related to VENABLE's drug trafficking activities is stored on iCloud in association with his Apple ID(s) and Apple Account(s). Therefore, I respectfully request that this Court issue the requested warrant.

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

50. The government will execute this warrant by serving the warrant on Apple.

Respectfully submitted,

Stacey Ivie
Taskforce Officer (TFO)
Drug Enforcement Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on October 13, 2020.

John F. Anderson

Digitally signed by John F. Anderson
Date: 2020.10.13 16:42:57 -04'00'

The Honorable John F. Anderson
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Apple Account(s) and Apple ID(s) associated with the following identifiers:

- TAUREAN VENABLE
- Cellular phone number 202-733-0357

that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California, 95014 in the Northern District of California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2018 through the present including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2018 through the present including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of Title 21, United States Code, Sections 841 and 846 involving Taurean Venable ("VENABLE") or any of his co-conspirators since January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the distribution of illegal drugs, communications between VENABLE and his co-conspirators, the identities of co-conspirators both within the Eastern District of Virginia and elsewhere, and other information constituting evidence, fruits, and/or instrumentalities of the above-described offense, including the following:

(a) The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

(b) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

(c) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

(d) Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

(e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple Inc.. The attached records consist of _____

_____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple Inc., and they were made by Apple Inc. as a regular practice; and

b. such records were generated by Apple Inc.'s electronic process or system that produces an accurate result, to wit: (1) the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple Inc. in a manner to ensure that they are true duplicates of the original records; and (2) the process or system is regularly verified by Apple Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature